International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume1, Issue 1 (April'2015)

DATA SECURITY IN CLOUD COMPUTING – A REVIEW

D.Gnanavelu,
Research Scholars,
Computer Science, Meenakshi University,
K.K Nagar, Chennai-78, Tamil Nadu, India

Dr. G.Gunasekaran ,
Principal,
Meenakshi College of Engineering,
K.K Nagar, Chennai-78, Tamil Nadu, India

ABSTRACT: Cloud computing is a promising and emerging technology for the next generation of IT applications. Cloud computing gained attention due to the growth of internet technologies, reduced costs of storage and processing, growth technologies of visualization and advancement in internet security. Cloud computing data security is one of the main challenges in cloud computing. An organization can decide to adopt cloud only on based on benefits to risk ratio. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This paper is focused on the security issues of cloud computing

Key words: Cloud Computing, cloud model, Cloud services, Data security issues, Cloud data Security

1. INDRODUCTION

Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements [1].

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(eg. networks, servers, storage, applications & services) that can be rapidly provisioned and released with minimal management effort or service provider interaction through internet. The Internet cloud works as a service factory built around virtualized data centers. Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. The idea is to migrate desktop computing to a service-oriented platform using virtual server clusters at data centers. In Cloud Computing, service providers provide the storage for data along with services. But due the lack of proper security policies, Cloud Computing adoption is becoming a serious issue. This paper primarily discusses various issues and possible solution to data security related issues.

2. CLOUD COMPUTING

Cloud computing is a computing model in which hardware, platform, infrastructure and software are defined and delivered as a service rather than a product. Cloud computing is emerging from recent advances in technologies such as hardware virtualization, Web services, distributed computing, utility computing and system automation. Cloud computing takes advantage of hardware virtualization to securely and dynamically allocate physical resources such as computational power, storage, and networks to the users. Cloud resources are are delivered to the end-users through Web services. Google proposed cloud computing concept in 2007, which would be including different business related services like Infrastructure as a Service (or "IaaS"), Platform as a Service (or "PaaS"), and Software as a Service (also known as "SaaS")[3].

2.1.CLOUD SERVICES

The services provided by cloud computing could be broadly categorized into 3 main categories.

1. Software as a service (SaaS)
2. Platform as a service (PaaS)
3. Infrastructure as a service (IaaS)

2.1.1 Software as a service (SaaS): In the Software as a Service, the services and all the software are all dealt over the cloud. The service providers manage all the offered services and also, those applications could be used by us, without actually installing them on our machines, regardless of the place where that application is stored. One of the example of SaaS is web services interface. Here are some other applications: Social network ,Video processing, Office suites ,CRM, etc.

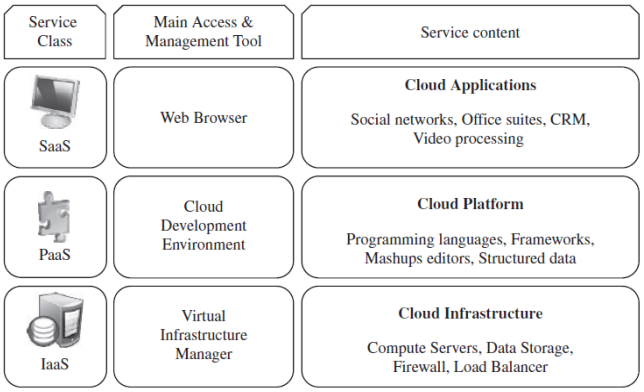

Fig.1. Cloud Services

2.1.2 Platform as a service (PaaS): PaaS here, is an another delivery model for application. It provides all the resources, which are required for building the applications and the various services over the internet without installing or downloading any actual software. This category is used for delivering system software like operating systems and other associated services, required to run the application, through cloud without being downloaded or installed.

2.1.3 Infrastructure as a Service or IaaS: Sometimes IaaS is also referred as HaaS or Hardware as a Service. It allows you to rent the resources like servers, storage, hardware, &other various networking hardware components. In this model of computing, users (Client/ Organization) outsource the above mentioned operations. The service providers of IaaS own the equipments. The providers are only in-charge of running and maintenance of these services. Clients only have to pay for the operations they use.

2.2 CLOUD MODEL

A cloud is basically a collection of different computers, anywhere in this world, with the functionality of paying-per-use only for the clouds being used. The different types of clouds which are there are as follows:

2.2.1 Private Clouds: The private clouds are basically the different datacenters whose use is been made in a private or secured network. It restricts the unwanted and unauthorized people to access the data that is under the company. This type of cloud is more secured than any other type of the traditional cloud. But, the managers will still have to take care of the purchase, building and maintenance work of the system.

2.2.2 Public Cloud : Public clouds follow the traditional ways and concepts of the cloud computing. It lets the users use the computing resources from any part of the world. The different services could be used in the same Pay-per-use method, means paying only for the services the user uses, not for the whole deal [9].

2.2.3 Hybrid Cloud: As per its name, a hybrid cloud or a mixed cloud is a mixture of both the clouds, i.e. the public and the private cloud. This is done by processing the work load through an enterprise data-center, and other services and activities would be provided by the help of a public cloud[9].

3. DATA STORAGE SECURITY ISSUES

Time, cost, innovation are great benefits of cloud computing but still there are significant security concerns of cloud computing that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. Major security issues related to those faced by cloud and security issues faced by their customers are discussed below:

3.1 **Abuse of Cloud Computing**: IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity often coupled with a frictionless registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

3.2 Account or Service Hijacking: Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

3.3 Unknown Risk Profile: One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns - complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications. Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas [2].

4. ALGORITHMS FOR DATA STORAGE SECURITY

4.1. RSA algorithm: Today RSA algorithm is one of the public key cryptography algorithms used for encryption and decryption by many vendors. This is the first generation algorithm that used for providing Security to data [8]. It can encrypt a message without the need to exchange a separate secret key. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Party A1 can send an

encrypted message to party B1 without any prior secret keys exchange. A1 uses B1's public key to encrypt the message and B1 decrypts it using the private key, which only he knows. RSA can also be usd to sign a message, so A1 can sign a message using their private key and B1 can verify it using A1's public key [8]. The RSA algorithm contains three steps, namely key generation, encryption and decryption. Here is the generating of key process which first is choosing two random numbers p and q. Then the number n should be computed [17]:
$n = pq$.
Thereafter a function $\varphi(n)$ is computed: $\varphi(n) = (p-1)(q-1)$.
Also an integer e is chosen so that $1 < e < \varphi(n)$.
Finally, the value of d is calculated: $d = e\text{-}1 \bmod \varphi(n)$, such that: $de \bmod \varphi(n) = 1$, and e and $\varphi(n)$ are co-prime. The result (n, d) is the private key and (n, e) is the public key.
Encryption a text m is calculated by: $c = me \bmod n$, and decryption a text is calculated by: $m = cd \bmod n$ [9].

6.1.1. RSA algorithm's Security : There are a lot of initial attacks on RSA, which are not so powerful, because there are improvements added to RSA, but one of the most famous one of these improvements is on use of common modulus for all users, for example not to choose different n = pq for each user. This problem can occur in a system, where a trusted central authority generates public and private keys for users by using a fixed value for n. In this case user A_1 can factor the modulus n, using his own exponents, e and d. Then A_1 can use the public key of B_1 to recover his private key. The solution is simply not to use a different n for each user. This attack is not applicable in systems, where each user generates the pair of keys on his/her machine. Here the value of n must be different for each user [17]. One of other attacks on RSA is called timing attack. When a user A1 uses RSA algorithm for digital signature or encryption/decryption, a troublemaker can specify the private key by measuring the time it takes to execute signature or decryption. This attack could be applied on the systems that are connected to a network, for example, using a smart card. The intruder cannot read the smart card's content, because it is resistant to unauthorized access, but he can determine the private key by using timing attack. One of the possibilities to Deal with timing attack is to add some delay to the process, because the process always takes a fixed amount of time [17].

5. CONCLUSION

Security of data in cloud is one of the major issue in cloud computing environment. This paper surveyed the various existing security measures in cloud computing and compare their various security parameters. To provide security of data in cloud is one of the major issues, which hold back the clients to store their data in cloud environment. Even though the security problems cannot be solved completely, better and powerful security measures can be applied to provide maximum security which can gain the trust of clients to store and access their data from the cloud storage.

REFERENCES

[1] N. Leavitt, "Is cloud computing really ready for prime time?" *Computer, vol. 42, no. 1, pp. 15–25, 2009.*

[2] Xiao D, Shu J, Chen K, Zheng W. A Practical Data Possession Checking Scheme for Networked Archival Storage. Journal of Computer Research and Development , *2009, 46(10) : 1660-1668*

[3] F. Soleimanian, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, *Vol. 1, ISSUE 6, pp. 49-54, 2012*

[4] Ateniese G, Kamara S, Katz J. Proofs of Storage from homomorphic identification protocols. In: Proc. Of ASIACRYPT *'09, 2009, pp. 319-333.*

[5] Ateniese G, Pietro R D, Mancini L V, Tsudik G. Scalable and efficient provable data possession. In: Proc. of SecureComm '08, *2008, pp.1-10.*

[6] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I.Brandic.―Cloud Computing and Emerging IT Platforms:Vision, Hype, and Reality for Delivering Computing as the 5th Utility,‖ Future Generation Computer Systems, *vol. 25, no. 6, June 2009, pp 599–616.*

[7] Farzad Sabahi, "Cloud Computing Security Threats and Responses", *978-1-61284-486-2, IEEE, 2011, pp: 245 – 249.*

[8] Ravi Gharshi, Suresha, "Enhancing Security in Cloud Storage using ECC Algorithm", International Journal of Science and Research (IJSR), *Vol 2, Issue 7, 2013.*

[9] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical Editor Bill Meine, Elsevier Publishing, 2011.

[10] Priyanka Arora, Arun Singh, Himanshu Tyagi ―Analysis of performance by using security algorithm on cloud network‖ in international conference on Emerging trends in engineering and management (*ICETM2012), 23-24 June, 2012*

[11] Vaishali Singh, S. K. Pandey, " Revisiting Cloud Security Issues and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering, *Volume 3, Issue 7, July 2013 ISSN: 2277 128X*

[12] M. Jensen, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, *pp: 109 – 116.*

[13] Z. Mahmood, "Data location and security issues in cloud computing," in *Proceedings of the 2nd International Conference on Emerging Intelligent Data andWeb Technologies* (EIDWT '11), pp. 49–54, IEEE, September 2011.

[14] IAIK - TU Graz : AES Lounge, http://www.iaik.tugraz.at/content/research/krypto/aes/#security [*accessed: 9 August 2013]*.

[15] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore *2009, pp. 109-116.*

[16] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities", IEEE, *1540-7993/11, 2011, pp: 50-57.*

[17] Abbas Amini, Secure Storage in Cloud Computing, Master Thesis, Technical University of Denmark, Kongens Lyngby, Denmark, 2012.

[18] S. Subashini ,V. Kavitha , "A survey on security issues in service delivery models of Cloud computing," Journal of Network and Computer Applications, *2011, pp.1-11*.

[19] M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.

AUTHOR PROFILE

D.GNANAVELU is a research scholar working in Meenakshi College of Engineering, Chennai He Received M.Phil(Computer Science) Degree in 2008 from Alagappa University India. His areas of interest are Networking and Cloud computing.

Dr.G.Gunasekaran received the B.E. degree in Computer Science from Madurai Kamarajar University, tamilnadu, india, in 1989, and the M.E. degree in Computer Science from Jadavpur University, in 2001. He received the Ph.D. degree in Data Mining at the Jadhavpur University, Kolkata , India in 2009. His interests include network coding, network measurements and security and Data Mining.